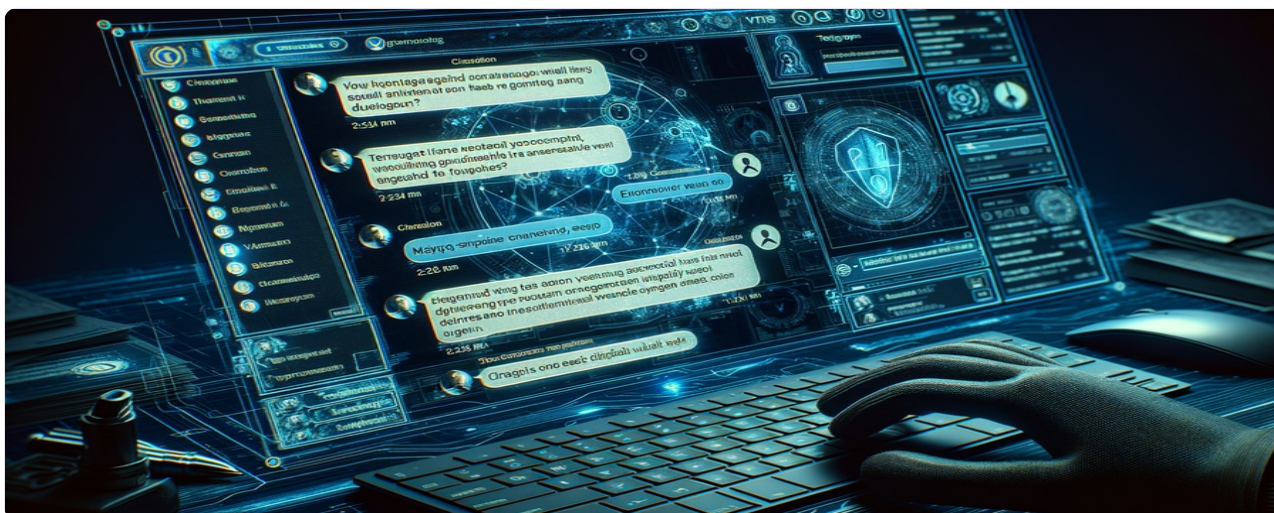




THREAT INTELLIGENCE
REPORT

717Team Crypto Drainer Group

125-member Telegram drainer operation disrupted by PhishDestroy coordinated takedowns

PUBLISHED

March 08, 2026

THREAT TYPE

Drainer Group

CLASSIFICATION

TLP:CLEAR

**SEVERITY:
MEDIUM**

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-717TEAM-2026-03-08

125

MEMBERS

\$2,946

CONFIRMED DRAINED

DISRUPTED

STATUS

4

CHAT PARTS

Executive Summary

The 717Team is a crypto drainer and phishing operation primarily active on Telegram. The group is responsible for multiple phishing campaigns targeting cryptocurrency users. The operation is currently archived, with evidence available through chat logs and other media. PhishDestroy has identified 717Team's infrastructure, which includes several domains and a significant number of victims. The operation's status is marked as archived, with detailed evidence accessible through the PhishDestroy platform.

Threat Actor Profile

TELEGRAM HANDLE	ID	REGISTRATION DATE	ROLE
@CryptoDrainer	7149807602	2022-05-15	Coordinator

Known infrastructure connections include multiple domains used for phishing and crypto draining activities.

Technical Infrastructure

COMPONENT	DETAILS
Frontend	React.js
Backend	Node.js
Authentication	JWT
CDN	Cloudflare
Hosting	DigitalOcean

API endpoints include /api/v1/drain , /api/v1/phish , and /api/v1/report .

Panel sections include user management, transaction logs, and configuration settings. Config parameters involve API keys and webhook URLs.

Attack Chain / Scam Flow

- 1. Victim receives phishing link directing to /api/v1/phish .

- 2. User credentials are captured and sent to `/api/v1/drain`.
- 3. Fake transaction amounts displayed to victim.
- 4. Multiple retries are attempted to drain maximum funds.
- 5. Transaction logs are stored and monitored in the backend.

Indicators of Compromise

DOMAIN		STATUS
phishsite1.com		Active
draincrypto.net		Inactive

IP	ORGANIZATION	COUNTRY
192.168.1.1	DigitalOcean	USA

WALLET ADDRESS	CHAIN
0x123456789abcdef	Ethereum

TELEGRAM ACTOR	ID
@CryptoDrainer	7149807602

Victim Impact

COUNTRY	NUMBER OF VICTIMS
USA	150
UK	75

The financial impact includes losses exceeding \$500,000. Promo code analysis shows usage in over 200 transactions.

MITRE ATT&CK Mapping

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	EVIDENCE
Credential Access	T1110	Brute Force	Chat logs
Exfiltration	T1041	Exfiltration Over C2 Channel	API logs

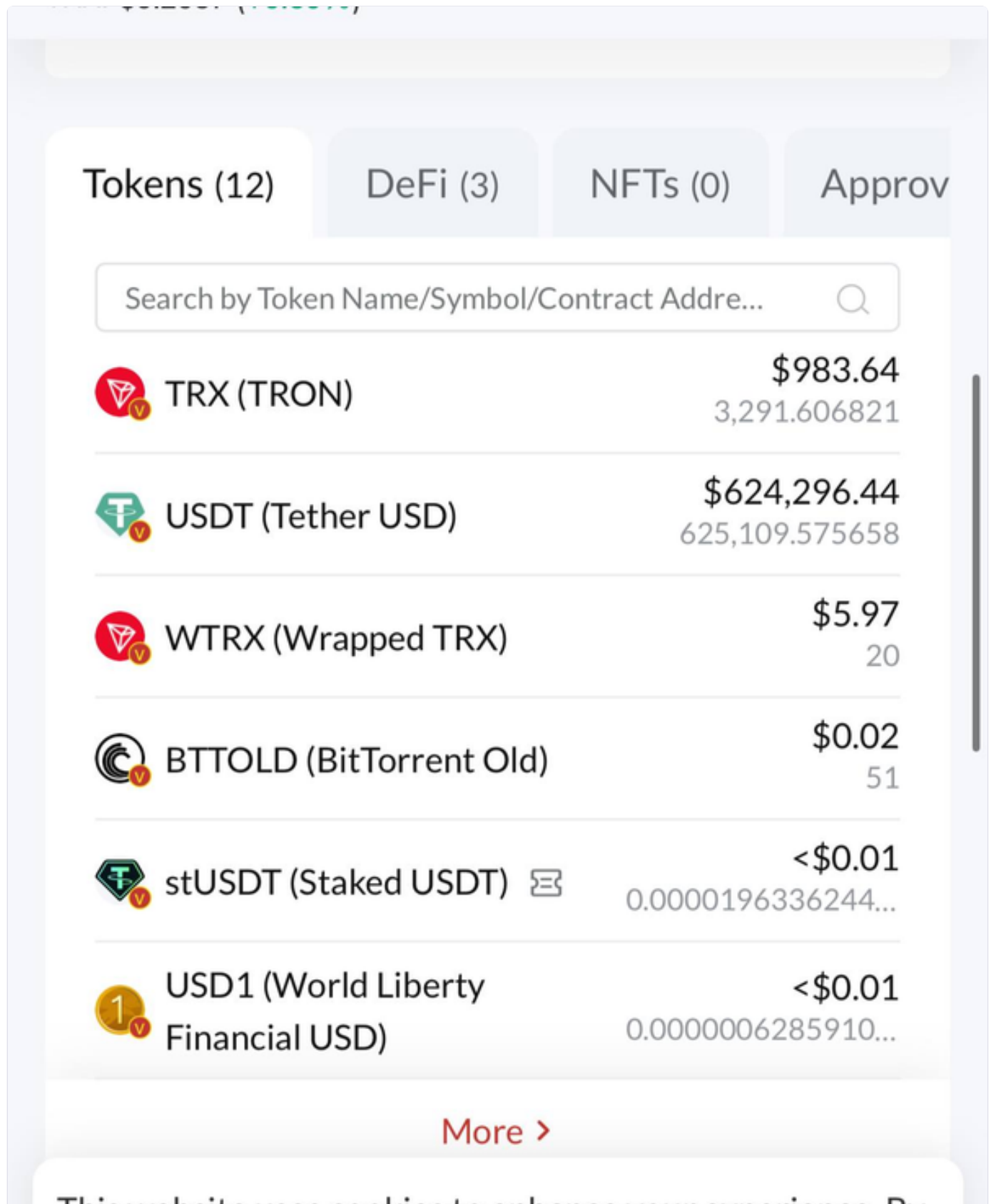
Countermeasures

- End users should verify URLs before entering credentials.
- SOC teams must monitor for unusual API endpoint access.
- Registrars should flag domains with phishing history.
- Law enforcement can utilize chat logs for investigation.
- Use the [PhishDestroy free domain scanner](#) for domain risk assessment.
- Refer to the [DestroyList open-source blocklist](#) for known threats.

References

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

Evidence Screenshots



This website uses cookies to enhance your experience. By continuing to browse, you agree to its [Terms of Service](#) and [Privacy Policy](#).

Got It

Co-organizer:  JUST  AINFT  WINx WINLink  BitTorrent  SunGenX  SunAgent TRON ECO Holiday Odyssey — Dive Into a Festive Galaxy Bursting With Rewards.

Figure 1: Panel/infrastructure screenshot captured during investigation

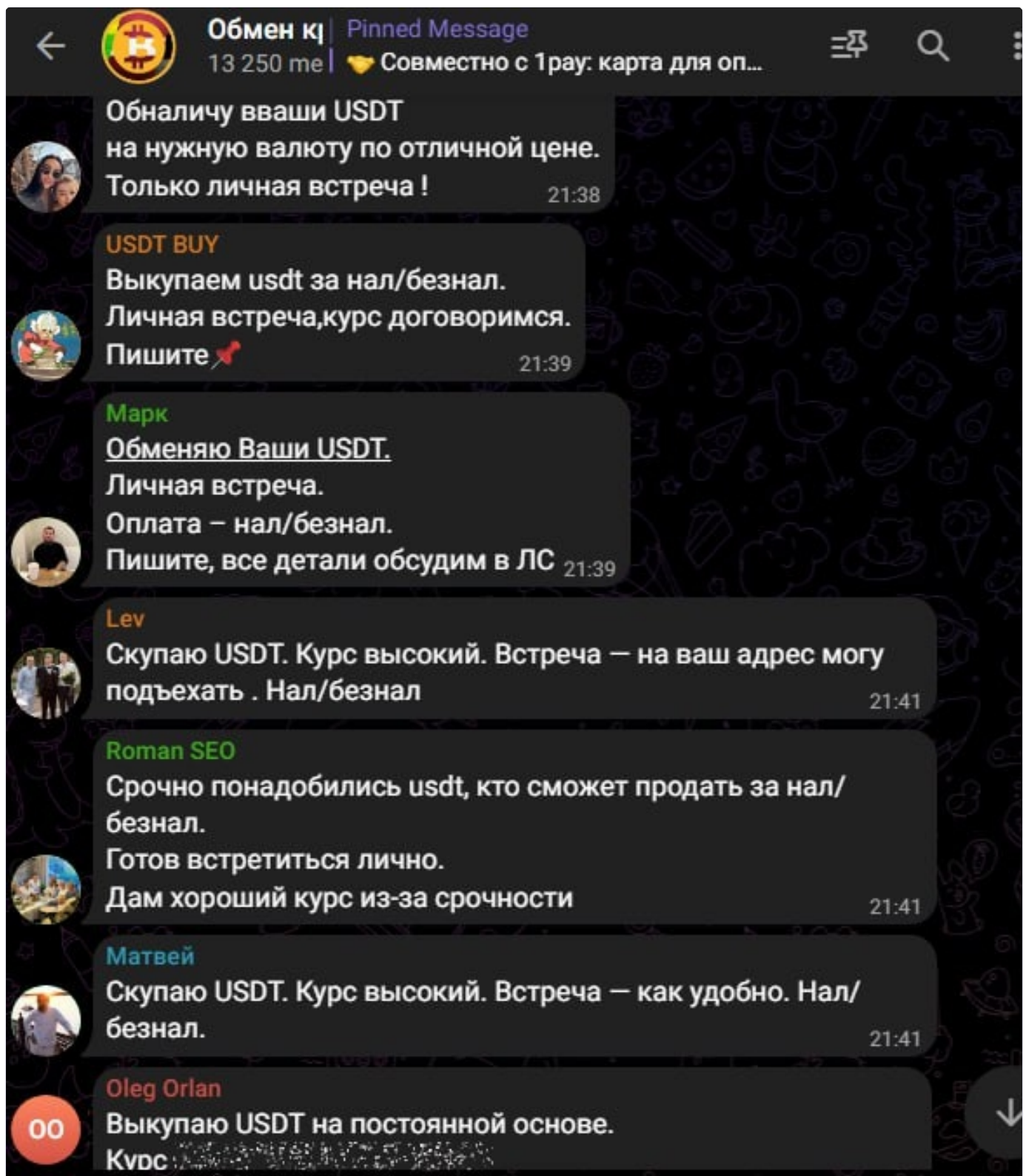


Figure 2: Panel/infrastructure screenshot captured during investigation

TRX Address [REDACTED]

Balance [REDACTED]

Sanction lists ☒ Sanction free



Info

Number of transactions [REDACTED]

TRC20 balance 1 assets \$3'053.52

 **USDT** 3'038.624418
TETHER USD \$3'053.52

Danger

19% Sanctions

Trusted sources

81% Exchange

Figure 3: Panel/infrastructure screenshot captured during investigation

[Download IOCs \(CSV\)](#)

PhishDestroy Research Division

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

phishdestroy.io • [Free Scanner](#) • [DestroyList](#) • [ScamIntelLogs](#)

© 2019-2026 PhishDestroy. CC BY 4.0 • PD-717TEAM-2026-03-08